Personnel Safety Interlocks

Introduction

Interlocks are used at LLNL to control numerous personnel and equipment hazards. Since interlocks are used in a wide variety of circumstances, it is not possible to prescribe a mandatory set of hardware or design specifications that force all interlock systems to be identical. However, human factors considerations dictate the establishment of minimum criteria to ensure that interlock systems work at least according to the same set of logic criteria. In particular, it is essential to ensure that–

- Interruption of interlock switches will automatically produce a safe condition.
- Similar safety instructions have roughly the same meaning.
- Basic emergency shutdown procedures follow the same general pattern.

This document is intended to provide guidance toward that end for interlock systems and for individual components. *Health & Safety Manual* Chapter 11 provides guidance for the level of sophistication in interlocking that any particular situation may require.

This supplement applies to new personnel safety interlock systems only. It does not require that integral interlocks on commercially available equipment be modified to meet the requirements of this supplement, or that existing personnel safety interlock systems be modified. If safety hazards are identified in existing interlock systems, however, upgrades should be designed to meet the requirements of this supplement. Finally, it is not intended to discourage the use of innovative technology in safety systems but only to ensure that the general philosophy of this supplement is followed so that the final system provides an equivalent level of safety.

General

The design for all interlock systems should incorporate the criteria enumerated in this section. This is not an exhaustive list, and it should be noted that additional requirements for specific interlock systems are listed elsewhere in the *Health & Safety Manual (H&SM)*. For additional criteria on interlocks to be installed in–

- Accelerator areas, see *H&SM* Section 33.48 and Supplement 33.48.
- Electrical areas, see *H&SM* Section 23.54.
- Laser areas, see *H&SM* Section 28.09.
- X-ray machines, see *H&SM* Section 33.47 and Supplement 33.47.

Automatic Safe Shutdown

Any breach of an interlock system should result in the automatic safe shutdown of the system in the shortest time interval possible, and to an acceptable personnel hazard level. Depending on the system and the level of hazard, this might mean disconnecting power, discharging capacitors, bleeding down pressure systems, returning radioactive material to shielded containers, etc.

Fail-Safe Operation

Components of interlock systems should be selected to ensure that either power interruption or the most likely mode of component failure will result in a safe shutdown of the system. When this cannot be reasonably ensured, redundant components are normally required. Examples are the installation of redundant interlock chains or dual interlock switches in series on the same door. When redundant circuits are used on interlock systems that employ programmable controllers, the redundant interlock circuits should be carried back to separate controllers.

Nonresetting

The act of making up an interlock chain must never, by itself, result in the starting or restarting of a piece of equipment. In general, once an interlock chain has been interrupted for any reason, it shall be necessary to repeat the entire sequence required to make up the interlock chain. In cases where the interlock system is composed of several sections (see below), it shall be necessary to make up the interlock chain for the section that was breached.

Wiring

Wherever possible, interlock systems should use low-voltage wiring. Where voltages in excess of 50 V are used, all wiring shall be in conduit or enclosed wireways as required by the National Electric Code (NFPA-70).

In general, conduits and trunk cables carrying interlock wiring should not contain conductors carrying power or signal voltages for other purposes. It is permissible, however, to route interlock cables in cable trays with other wiring, provided the mechanical and electrical integrity of the interlock cable is assured.

Within equipment enclosures, interlock wiring should be grouped separately from other wiring. Interlock wiring should not share the same terminals or cross-connect blocks with other wiring. Terminals and cross-connect blocks should be enclosed to discourage unauthorized interlock bypassing. It is also desirable to provide clear marking for all interlock cables and cross-connect terminals.

Where interlock wiring is bundled with other control wiring in the same cable or conduit, the other wiring shall not operate at voltages higher than that of the interlock wiring, and current must be limited to preclude damage to the interlock conductors in case of a short circuit.

Sectioning

Interlock systems that cover large areas or multiple facilities may be broken down into several sections. Sections may be swept separately, and breaking of one section's interlock chain need not require that the interlock chain in other sections be made up anew. Breaking of the interlock chain for a section must result in the automatic safe shutdown of that section.

Clearly, sections must cover appropriate areas, and completing the interlock chain for any section must not activate a hazard in any section where the interlock chain is not complete.

Configuration and Logic Analysis

The configuration of each interlock system shall be documented with approved schematics, wiring diagrams, drawings, and specifications as appropriate. The configuration documentation shall also include a logic analysis to ensure that the system works as intended and that the requirements of this document are met. For complex systems, fault tree analyses may be needed. For systems employing programmable controllers, the configuration documentation should include a review of the programming of the controllers. A formal review of the configuration documentation is required. The approved documentation shall be updated following modification. Proposed modifications or reprogramming of controllers require approval by the same management level that approved the original installation.

For some applications, it may be desirable to develop standard systems for which a logic analysis is done only once. An example would be a laser access control interlock system.

Testing

Each safety function of any interlock system shall be tested on initial installation; whenever modifications, repairs, or maintenance are complete; and when programmable controllers have been reprogrammed. Testing requirements can be kept to a minimum if dedicated programmable controllers are used for interlock systems, in particular where other functions require frequent reprogramming. In addition, each safety function of any interlock system shall be tested quarterly unless otherwise specified. The interlock check frequencies for x-ray machines and accelerators are specified in Section 33.47, "X-Ray Machines," and Supplement 33.48, "Uniform Accelerator Safety Standard," of the *Health and Safety Manual*. A written record shall be kept of each test made.

Interlock Bypassing for Maintenance and Troubleshooting

Bypassing interlocks for maintenance, troubleshooting, or any other reason shall be controlled by written safety procedures–i.e., Facility Safety Procedures or Operational Safety Procedures. This includes modifications of programming for programmable controllers to simulate interlock bypassing. The procedures shall address who may bypass interlocks, what supervision is required, muster provisions for personnel, communication with personnel in the area, maintenance of bypass logs ("bugger books"), etc., as appropriate.

When electrical hazards are present while work is done within interlocked enclosures or on interlocked systems, all provisions of the Electronics Engineering Department Electrical Safety Policy LED 61-00-01-AIA shall apply.

Whenever interlocks are bypassed, the interlock bypass condition shall be prominently identified at the console or master control and in the area where the hazard exists. In addition, interlock bypass conditions should be annunciated at other appropriate control or indicator panels. When interlocks are bypassed frequently, automatic indication is desirable; in other cases, posting of signs and placement of temporary warning beacons would be more appropriate.

Where at all possible, interlock bypassing shall be accomplished in a manner that is self-limiting. For example, this can be done through enclosure switches that are self-restoring when the doors are closed, through software instructions that expire at the end of the shift, or with captive key switches that inhibit full operation until the bypass condition is terminated.

Routine Interlock Bypassing

Where interlock systems are provided that limit access to an area to qualified personnel (as opposed to total exclusion of personnel), routine bypass features may be provided. Examples are bypass provisions at access doors to laser areas.

Bypass devices must be of the time-limited and self-resetting type. Bypassing of interlocks shall re-

quire a written safety procedure. When routine bypassing is authorized, the interlock chain must include circuitry to activate lights or other indicators at the console or master control unit in order to warn the operator of the bypass condition, and to remind him of the extra precautions to be taken. Indicating the bypass condition on other status indication devices should also be considered.

Components

All interlock components must provide protection for the same hazard or the same set of hazards, and violation of the interlock system must result in the same protective measure, regardless of which component was involved. Not all of the following components are required for all interlock systems, but where they are provided they must meet the following criteria:

Master Control

Each interlock system must have a master control that monitors the interlock system, enables the equipment when the entire interlock chain is made up, and initiates automatic safe shutdown of the system when the interlock chain is broken.

Status Indicators

At least one status indication device must be provided at the console where the hazardous equipment or process is controlled. Where personnel could conceivably be left in an interlocked area, status indicators that are clearly visible from all points within the interlocked area must also be provided within that area. Flashing lights, rotating beacons, and audible alarms may be needed to supplement status indicators in complex installations. Additional status indicators may also be desirable at entrances to the interlocked areas. When multiple status indicators are provided, the indicators must be coupled to assure that all indicators express the same condition when the interlock chain is broken or bypassed.

Each status indicator must provide positive identification of the system status. At the very least, "system enabled" and "system off" indications must be provided. Additional intermediate status levels can be provided as needed. Color coding for status indication shall follow the requirements of *H&SM* Chapter 11. Consult the Hazards Control safety team in the area for appropriate wording for status indication.

Lock-Controlled Master Switch

A Lock-Controlled Master (LCM) switch is the final link in an interlock chain. The hazardous equipment cannot be turned on unless the LCM switch has been turned on, and the LCM switch cannot be turned on unless all other interlock chain requirements have been satisfied. The LCM switch shall have only one key (or one set of keys, where multiple keys are required for machine actuation) that may be removed only when the switch is in the "off" position and the hazard has been deactivated. At times this is also referred to as a "captive key" system. LCM switches may not be bypassed and must be wired so that they cannot be bypassed easily.

LCM switches are recommended for any interlock system where positive control is desired. They are *required–*

- For interlock systems that contain sweep stations.
- For accelerator systems.
- For applications requiring temporary personnel access to areas where personnel are normally excluded, without breaking the entire interlock chain. Note that LCM key switch access is not appropriate for areas where routine bypass features have been installed. (See above.)

Sweep Stations

An interlocked area that is of sufficient size that personnel could inadvertently be left in the area shall have LCM key-operated sweep stations.

Making up the interlock chain shall require that each sweep station be activated with the LCM key in a specified sequence or within a suitable time limit, as appropriate. Sweep stations should be located so that the sweeper must tour the entire area, forcing him to look into every space where an individual might be located. Sweep stations shall not be bypassed by any remote or local means. Sweep procedures should include audible alarms or broadcast of voice warnings as appropriate.

Emergency Stop Buttons

An interlocked area that is of sufficient size that personnel could conceivably be left behind shall have emergency stop buttons. Enough stop buttons must be provided to ensure that a trapped individual can trip the interlock system and deactivate the equipment within a safe time span. Activation of the emergency stop button shall initiate the automatic safe shutdown; shall shift all status indicators to indicate a safe condition; and shall require that the entire interlock chain be

made up again before the equipment can be reenergized.

Status Control Stations

Status control stations are standard components for personnel safety interlock systems that are available from stores. They replace the Run-Safe boxes in use before 1987. Status control stations have been designed to meet the criteria for three separate components: status indicator, emergency stop button, and LCM sweep station. These units operate on 24 volts and meet all other LLNL criteria. The use of Status control stations is encouraged, but custom designed units are satisfactory as long as the components function as described here. Status control stations should be used only inside the controlled areas. Separate status indicators or area access control warning lights should be used at entrances to the interlocked area.

Run-Safe Boxes

Run-safe boxes are components of interlock systems formerly installed at LLNL. No new interlock systems should be designed that use these components, but a limited number of run-safe boxes are carried in stores stock for repair and minor extensions of existing interlock systems.

KJA/sh